## REMARKS

Claims 1 and 18 are currently amended. Claims 1-44 remain in the application. In view of the foregoing amendments and the following remarks, Applicant respectfully requests that the rejections be withdrawn and that the application be forwarded onto issuance.

### Claim Rejections under 35 U.S.C. § 101

Claims 1-17 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. The Office asserts that the step of "determination of pairings for use in an elliptic curve cryptography system" fails to establish a concrete, useful, and tangible result. Applicant respectfully disagrees with the Office's argument, but amends claim 1 to recite "encrypting the selected information based on the pairings" to overcome the rejection.

Page 13 (lines 7-13) of the subject application expressly states that "[f]or example, methods and apparati are provided for use in **cryptographically processing information** based on elliptic and other like curves. The methods and apparati allow pairings, such as, for example, Weil pairings, Tate Pairings, Squared Weil pairings, Squared Tate pairings, and/or other like pairings to be determined based on algorithms that utilize a parabola. The methods and apparati represent an improvement over conventional algorithms since they tend to be more computationally efficient." (Emphasis added). These methods and apparati are beneficial in certain applications, such as generating product keys, where one wants product IDs that provide improved security with reduced computational cost. Applicant has added the step of encrypting data based on the cryptographic processing, and respectfully requests the Office to remove the rejection.

Claims 18-30 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. The Office asserts that its implementation can be performed solely by carrier wave mediums. Applicant respectfully disagrees. Nevertheless, without conceding the propriety of the Office's rejection and for the sole purpose of expediting allowance, this claim has been amended to recite "a computer-readable storage medium," (emphasis added), and as such the implementation cannot be performed solely by carrier wave mediums.

For at least this reason, these claim stands allowable.

**Claim Rejections under 35 U.S.C. § 112, First Paragraph**

Claims 1-44 stand rejected under 35 U.S.C. § 112, first paragraph, as based on a disclosure which is not enabling. Specifically, the Office asserts that the subject matter pertaining to how the pairings are employed towards the implementation of the elliptic curve cryptography system is not disclosed. Applicant respectfully points out that the specification describes improved pairing by combining two conventional computation steps for the Weil pairing or the Tate pairing and then describes simplifying computation of the result using parabolas. The improvement provided can also be used to compute the squared Weil pairing and the squared Tate pairing.

Since the specification is more than sufficient for a person skilled in the art to make and use the invention, Applicant respectfully requests that the 35 U.S.C. § 112, First Paragraph rejection be removed.

**Claim Rejections under 35 U.S.C. § 112, Second Paragraph**

Claims 4, 6, 11-17, 20, 24-30, 34, and 38-44 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Specifically, claims 13, 15, 17, 26, 28, 30, 40, 42, and 44 stand rejected for reciting a point Q as **Q** and **–Q**. Applicant respectfully submits that Q is a point defined in a field that lies on an elliptic curve (see page 15, line 13: "let: ... ***P***, ***Q***, ***R***, ***X*** be points on *E*"). Q is a mathematical variable representing a pair of numbers that map to a particular point on a field. Conceptually, a point on a field is similar to a point on a Cartesian plane, except the point maps to a field instead of the Cartesian plane. Therefore, in response to the Office's question, Q is not a vector. In response to the Office's question, multiplying Q by -1 does imply a scalar multiplication on both of Q's coordinates.

Claims 11, 24, and 38 stand rejected for the same reasons as Claim 13, and for reciting a "multiple of a point". Applicant respectfully submits that a point on a finite field can be added to itself some number of times, and the result is called a "multiple of a point," a term that is well known in the art.

Claims 12, 14, 16, 25, 27, 29, 39, 41, and 43 stand rejected because the Office asserts it is uncertain what j, k, the parabolic function, lambda, and the subscripted variables refer to.

Applicant respectfully submits that variables j and k are integers used to index the family of functions *f*. Together with point ***P***, integer variables j and k indicate which particular function in the family of functions is being referred to. These are subscripts are labels, not parameters. $f_{j,\boldsymbol{P}}(\boldsymbol{X})$ and $f_{k,\boldsymbol{P}}(\boldsymbol{X})$ are functions of one variable ($\boldsymbol{X}$) built using point ***P***. $f_{j,\boldsymbol{P}}(\boldsymbol{X})$ and $f_{k,\boldsymbol{P}}(\boldsymbol{X})$ are the $j^{th}$ and $k^{th}$ function in a series of functions that are recursively computed on the way to computing the final function, which will evaluate to the pairing.

The Office asserts that Claim 12 introduces two more variables without clarification, lowercase x and lowercase y. Applicant respectfully submits that variables $x$ and $y$ are the true variables of the function being constructed. The function $f$ is a function of a point $\boldsymbol{X}$; $x$ and $y$ represent the x and y coordinates of $\boldsymbol{X}$.

The Office asserts that Claim 12 recites undefined and consequently indefinite subscripted variables $x_4$ and $y_4$. Applicant respectfully submits that $x_4$ and $y_4$ are defined in Claim 12: "$-2j\boldsymbol{P}-k\boldsymbol{P}=(x_4,y_4)$." This equation implies that given a point ***P*** and integers $j$ and $k$, one can compute $-2j\boldsymbol{P}-k\boldsymbol{P}$, which when evaluated yields $(x_4,y_4)$.

The Office asserts that Claim 14 recites a variable, lambda, which is undefined. Applicant respectfully submits that lambda is defined as the slope of a

line through points $j\boldsymbol{P}=(x_1,y_1)$, $k\boldsymbol{P}=(x_2,y_2)$ and $j\boldsymbol{P}+k\boldsymbol{P} = (x_3, y_3)$ (page 22 lines 12-13). This slope is used to define a parabola which is used to construct iterations of the function $f$, which is used to calculated Weil and Tate pairings.

The Office asserts that the parabola recited in Claim 12 is undefined. Applicant respectfully submits that the parabolic function recited in claim 12 is defined, with the definition operator ":=", in the specification (page 23, lines 9-10):

$$\text{parab}(\boldsymbol{X}) := (x(\boldsymbol{X}) - x_1)(x(\boldsymbol{X}) + x_1 + x_3 + a_2 + \lambda_1 \lambda_2) + (\lambda_1 + \lambda_2 + a_1)(y_1 - y(\boldsymbol{X}))$$

The Office asserts that the parabola recited in Claim 14 (parab ($\boldsymbol{X}$) := $(x(\boldsymbol{X}) - x_1)(x(\boldsymbol{X}) + x_1 + x_3 + a_2 + \lambda_1 \lambda_2) + (\lambda_1 + \lambda_2 + a_1)(y_1 - y(\boldsymbol{X}))$) is undefined because it is defined in terms of variables whose values and meanings are undefined. Applicant respectfully submits that $\lambda_1$ and $\lambda_2$, $a_1$ and $a_2$, and $x_1$, $x_3$, and $y_1$ are defined in the specification.

Applicant respectfully submits that $\lambda_1$ and $\lambda_2$ are defined in the specification (page 22, lines 15 and 23 respectively) as:

$$\lambda_1 = \frac{y_1 - y_2}{x_1 - x_2} = \frac{y_1 - (-y_3 - a_3 - a_1 x_3)}{x_1 - x_3}$$

$$\lambda_2 = \frac{y_1 - y_4}{x_1 - x_4} = \frac{y_1 - y_3}{x_1 - x_3}$$

Applicant respectfully submits that $a_1$ and $a_2$ are constants of the $xy$ and $x^2$ terms of the ellipse equation defined in the specification (page 22 lines 12-14) as:

$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$

Finally, Applicant respectfully submits $x_1$, $x_3$, and $y_1$ are defined in the specification (page 22 lines 12-13):

$j\boldsymbol{P}=(x_1,y_1)$, $k\boldsymbol{P}=(x_2,y_2)$ and $j\boldsymbol{P}+k\boldsymbol{P}=(x_3, y_3)$.

Given point $\boldsymbol{P}$ and integer $j$, $k$, or both $j$ and $k$, these equations evaluate to points which define $x_1$, $x_3$, and $y_1$.

The Office asserts that there is a difference between the ":=" operator and the "=" operator. Applicant respectfully submits that ":=" is the definition operator – this operator is used when a relationship is first established. Definition of a relationship does not refer to a singular assignment, but rather refers to a definition. The equality operator ("=") is used to recite a relationship between functions that have already been defined. Claim 14 recites the definition of a parabola using the ":=" operator because the parabola is being defined for the first time. Claim 12 on the other hand recites a relationship between functions that have already been defined ($f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X})-x_4)}$), and so the traditional "=" operator is used. In all cases the operators are referring to mathematical relationships.

The Office asserts that the attributes of the field and the elliptic curve must be defined. Applicant respectfully submits that elliptic curve E is defined on page 15, line 10: "Let $E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over a field $K$." To one of ordinary skill in the art of Elliptic Curve Cryptography, the

"field" over which the ellipse is defined is a finite field. For background, see http://en.wikipedia.org/wiki/Elliptic_Curve_Cryptography.

The Office asserts that it is uncertain what is referred to by the term "Squared Tate" pairings and "Squared Weil" pairings. Applicant respectfully submits that Weil and Tate pairings are well-known in the art. A "Squared Weil pairing" is further defined on page 17, lines 7-12, and the "Squared Tate pairing" is further defined on page 19, lines 16-24.

Thus, Applicant respectfully requests that the 35 U.S.C. §112 second paragraph rejection of claims 4, 6, 11-17, 20, 24-30, 34, and 38-44 be removed.

**Claim Rejections under 35 U.S.C. §102(e)**

Claims 1-3, 5, 7-10, 18, 19, 21-23, 31-33, and 35-37 stand rejected under 35 U.S.C. §102(e) as being anticipated by Lenstra.

**The Claims**

**Claim 1**, as amended, recites a method for use in curve-based cryptography, the method comprising:

- determining a curve for use in cryptographically processing information;
- determining pairings for cryptographically processing said information using a parabola associated with said curve; and
- encrypting the selected information based on the pairings.

In making out a rejection of this claim, the Office argues that the subject matter is anticipated by Lenstra. Applicant respectfully disagrees and traverses the rejection. Claim 1 recites "determining pairings for use in cryptographically processing said selected information by selectively using at least one ***parabola*** associated with said at least one curve." While Lenstra appears to disclose participants choosing an elliptic curve from a predetermined set of elliptic curve equations, and Lenstra discloses participants choosing a finite field, Lenstra does not disclose using a parabola associated with the elliptical curve to determine pairings as is recited in Claim 1. Specifically, Lenstra does not disclose a method of calculating pairings, and Lenstra does not disclose a parabola – for determining pairings or for any other reason.

Since Lenstra does not recite each and every element of Applicant's claim 1, Applicant respectfully requests that the 35 U.S.C. §102(e) rejection be removed, and Applicant suggests that claim 1 is now in condition for allowance.

**Claims 2-17** depend from claim 1 and, as such, the remarks made above in regards to claim 1 apply equally to these claims. The rejections of these claims are also improper as failing to show these claims'

**Claim 18**, as amended, recites a computer-readable storage medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

- determining at least one curve for use in cryptographically processing selected information;
- calculating pairings for use in cryptographically processing said selected information by selectively using at least one parabola associated with said at least one curve; and

- cryptographically processing said selected information based on said pairings.

In making out a rejection of this claim, the Office argues that the subject matter is anticipated by Lenstra. Applicant respectfully disagrees and traverses the rejection. Claim 18 is not anticipated by Lenstra for the same reasons Claim 1 is not anticipated by Lenstra – Lenstra does not disclose "calculating pairings for use in cryptographically processing said selected information by selectively using at least one ***parabola*** associated with said at least one curve."

For at least this reason, Applicant respectfully requests that the rejection of claim 18 be removed, and suggests that claim 18 is now in condition for allowance.

**Claims 19-30** depend from claim 18 and, as such, the remarks made above in regards to claim 18 apply equally to these claims.

**Claim 31** recites an apparatus comprising:

- memory configurable to store information; and
- logic operatively coupled to said memory and configurable to at least support cryptographic processing of selected information stored in said memory by determining at least one curve for use in cryptographically processing selected information and determining pairings for use in cryptographically processing said selected information by selectively using at least one parabola associated with said at least one curve.

In making out a rejection of this claim, the Office argues that the subject matter is anticipated by Lenstra. Applicant respectfully disagrees and traverses the rejection. Claim 31 is not anticipated by Lenstra for the same reasons Claim 1 is not anticipated by Lenstra – Lenstra does not disclose "calculating pairings for use

in cryptographically processing said selected information by selectively using at least one ***parabola*** associated with said at least one curve."

For at least these reasons, Applicant respectfully suggests that claim 31 is in condition for allowance.

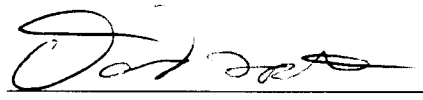
**Claims 32-44** depend from claim 31 and, as such, the remarks made above in regards to claim 31 apply equally to these claims.

**Conclusion**

All of the claims are now in condition for allowance. Accordingly, Applicant requests a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Respectfully Submitted,

Dated: 10-8-2007

By: 

David W. Foster
Reg. No. 60,902
(509) 324-9256 ext 219